IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of:	Date: June 12, 2007
Satoshi HADA, et al.	Confirmation No. 9214
Serial No: 10/651,691	Group Art Unit: 2168
Filed: August 29, 2003	Examiner: Dangelino N. GORTAYO

For: METHOD AND SYSTEM FOR PROVIDING PATH-LEVEL ACCESS CONTROL FOR STRUCTURED DOCUMENTS STORED IN A DATABASE

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir or Madam:

Appellant submits this Appeal Brief pursuant to the Notice of Appeal filed in this case on February 14, 2007.

I. REAL PARTY IN INTEREST

The real party in interest is International Business Machines Corp. of Armonk, New York by virtue of an assignment from the inventor(s) recorded in the U.S. Patent and Trademark Office on August 29, 2003, at Reel No. 014457, Frame No. 0947.

II. RELATED APPEALS AND INTERFERENCES

There are no appeals, interferences, or judicial proceedings known to Appellant, the Appellant's legal representative, or Assignee, which may be related to, directly affect, be directly

affected by, or have a bearing on the decision by the Board of Patent Appeals and Interferences in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-37 have been rejected. Appeal is taken from the rejection of claims 1-37.

IV. STATUS OF AMENDMENTS

No amendments were filed subsequent to the final Office action dated November 14, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to "an improved method and system for providing path-level access control for structured documents stored in a database" (pg. 5, lns. 6-7). In the present invention, "a structured document is parsed into a plurality of nodes that form a node tree. Each node is then associated with a path that describes the node's hierarchical relationship to its parent node(s). A translator receives an access control policy for the structured document that comprises at least one access control rule, and generates for each path a corresponding value expression based on the access control policy. The value expression is a simple statement granting or denying access to the node associated with the path" (pg. 5, lns. 16-22).

Independent claim 1 recites a method for controlling access to structured documents. The method includes providing an access control policy (107) for a structured document comprising a plurality of nodes, wherein the access control policy (107) comprises a plurality of access control rules. *See, e.g.*, pg. 8, lns. 1-11; fig. 1. The method also includes generating a path for each of

the plurality of nodes in the structured document (306). *See, e.g.*, pg. 8, lns. 19-21; fig. 3. The method further includes generating a value expression for each path based on at least one of the plurality of access control rules (308), wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document. *See, e.g.*, pg. 9, lns. 20-26; fig. 3.

Independent claim 11 recites a computer readable medium encoded with a computer program for controlling access to structured documents. The computer program includes instructions for providing an access control policy (107) for a structured document comprising a plurality of nodes, wherein the access control policy (107) comprises a plurality of access control rules. *See, e.g.*, pg. 8, lns. 1-11; fig. 1. The computer program also includes instructions for generating a path for each of the plurality of nodes in the structured document (306). *See, e.g.*, pg. 8, lns. 19-21; fig. 3. The computer program further includes instructions for generating a value expression for each path based on at least one of the plurality of access control rules (308), wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document. *See, e.g.*, pg. 9, lns. 20-26; fig. 3.

Independent claim 21 recites a computer system for controlling access to structured documents. The computer system (104) includes a database management system (105) implemented on the computer system (104). *See, e.g.*, pg. 6, ln. 18 to pg. 7, ln. 1; fig. 1. The database management system (105) includes an access control policy (107) for a structured document, wherein the structured document comprises a plurality of nodes and the access control policy (107) comprises a plurality of access control rules. *See, e.g.*, pg. 8, lns. 1-11; fig. 1. The

database management system (105) also includes an access control mechanism (200) configured to generate a path for each of the plurality of nodes in the structured document and generate a value expression for each path based on at least one of the plurality of access control rules, wherein the value expression is an executable statement utilized by the database management system during access control evaluation to determine whether a user is allowed to access a node in the structured document. *See, e.g.*, pg. 8, lns. 19-21; pg. 9, lns. 20-26; figs. 2-3.

Independent claim 30 recites a method for controlling access to structured documents. The method includes providing an access control policy (107) for a structured document comprising a plurality of nodes, wherein the access control policy (107) comprises a plurality of access control rules. *See, e.g.*, pg. 8, lns. 1-11; fig. 1. The method also includes generating a path for each of the plurality of nodes in the structured document (306). *See, e.g.*, pg. 8, lns. 19-21; fig. 3. In addition, the method includes generating a value expression for each path based on at least one of the plurality of access control rules (308), wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node. *See, e.g.*, pg. 9, lns. 20-26; fig. 3. The method further includes storing each path and the corresponding value expression in a table (310), wherein the value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document. *See, e.g.*, pg. 16, ln. 36 to pg. 17, ln. 8; fig. 3.

Independent claim 33 recites a computer readable medium encoded with a computer program for controlling access to structured documents. The computer program includes instructions for providing an access control policy (107) for a structured document comprising a plurality of nodes, wherein the access control policy (107) comprises a plurality of access control

rules. *See, e.g.*, pg. 8, lns. 1-11; fig. 1. The computer program also includes instructions for generating a path for each of the plurality of nodes in the structured document (306). *See, e.g.*, pg. 8, lns. 19-21; fig. 3. In addition, the computer program includes instructions for generating a value expression for each path based on at least one of the plurality of access control rules (308), wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node. *See, e.g.*, pg. 9, lns. 20-26; fig. 3. The computer program further includes instructions for storing each path and the corresponding value expression in a table (310), wherein the value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document. *See, e.g.*, pg. 16, ln. 36 to pg. 17, ln. 8; fig. 3.

Independent claim 36 recites a method for controlling access to structured documents. The method includes providing an access control policy (107) for a structured document comprising a plurality of nodes, wherein the access control policy (107) comprises a plurality of access control rules. *See, e.g.*, pg. 8, lns. 1-11; fig. 1. The method also includes generating a path for each of the plurality of nodes in the structured document (306). *See, e.g.*, pg. 8, lns. 19-21; fig. 3. In addition, the method includes generating a value expression for each path based on at least one of the plurality of access control rules (308). *See, e.g.*, pg. 9, lns. 20-26; fig. 3. The generating step includes normalizing each of the access control rules into a format comprising a head, a path and a condition (402), wherein the condition indicates who is granted or denied access to the path and under what circumstances. *See, e.g.*, pg. 9, ln. 27 to pg. 10, ln. 1; fig. 4. The generating step also includes propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule

(406). *See, e.g.*, pg. 10, ln. 17 to pg. 11, ln. 2; fig. 4. The generating step further includes transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path (410). *See, e.g.*, pg. 13, lns. 5-9; fig. 4. The method further includes storing each path and the corresponding value expression in a table (310), wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document. *See, e.g.*, pg. 16, ln. 36 to pg. 17, ln. 8; fig. 3.

Independent claim 37 recites a computer readable medium encoded with a computer program for controlling access to structured documents. The computer program includes instructions for providing an access control policy (107) for a structured document comprising a plurality of nodes, wherein the access control policy (107) comprises a plurality of access control rules. *See, e.g.*, pg. 8, lns. 1-11; fig. 1. The computer program also includes instructions for generating a path for each of the plurality of nodes in the structured document (306). *See, e.g.*, pg. 8, lns. 19-21; fig. 3. In addition, the computer program includes instructions for generating a value expression for each path based on at least one of the plurality of access control rules (308). *See, e.g.*, pg. 9, lns. 20-26; fig. 3. The generating instruction includes normalizing each of the access control rules into a format comprising a head, a path and a condition (402), wherein the condition indicates who is granted or denied access to the path and under what circumstances. *See, e.g.*, pg. 9, ln. 27 to pg. 10, ln. 1; fig. 4. The generating instruction also includes propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule (406). *See, e.g.*, pg. 10, ln. 17 to pg. 11, ln. 2; fig. 4. The generating instruction further includes transforming each of the at least one access control

rules affecting each path into a statement indicating who is granted and denied access to the path (410). *See, e.g.*, pg. 13, lns. 5-9; fig. 4. The computer program further includes instructions for storing each path and the corresponding value expression in a table (310), wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document. *See, e.g.*, pg. 16, ln. 36 to pg. 17, ln. 8; fig. 3.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Appellant requests review as to claims 1-37, and their rejection under 35 U.S.C. § 102(b) as being anticipated by "A Fine Grained Access Control System for XML Documents" by Damiani et al. (hereinafter "Damiani").

VII. ARGUMENTS

1. Claims 1, 11, 21, 30, 33, and 36-37 Are Not Anticipated by Damiani

Claim 1 recites a method for controlling access to structured documents. The method includes providing an access control policy for a structured document comprising a plurality of nodes, wherein the access control policy comprises a plurality of access control rules, generating a path for each of the plurality of nodes in the structured document, and generating a value expression for each path based on at least one of the plurality of access control rules, wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

Damiani does not disclose, teach, or suggest the claimed subject matter.

Damiani is directed to "a fine-grained access control system for XML documents" (title). In Damiani, "an access control model . . . that . . . allows the definition and enforcement of access restrictions directly on the structure and content of the documents" is presented (abstract).

(A)(i) Damiani does not disclose, teach, or suggest "generating a value expression for each path based on at least one of the plurality of access control rules, wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document"

Damiani does not disclose, teach, or suggest "generating a value expression for each path based on at least one of the plurality of access control rules, wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document," as recited in claim 1.

In the final Office action, the Examiner states:

> Damiani teaches . . . "generating value expression for each path based on at least one of the plurality of access control rules," (pg. 186, Section 5.2 "Access Authorization" and Figure 5, wherein access authorizations express the requirement of access for each path of the object) "wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document." (pg. 186, Example 5.1, Figure 5, and Algorithm 6, wherein the "Sign" column indicates the authorization for objects, as indicated by a path expression, that a user holds, as indicated in the subject column. A user is given authorization after Algorithm 6 is executed, determining the view returned to a given user accessing an object.

(November 14, 2006 final Office action, pgs. 2-3).

The Examiner also states in the final Office action:

> a. Applicant's argument is stated as Damiani does not disclose that "access authorization" is an executable statement.
>
> In response to the argument, Examiner respectfully disagrees. In the Damiani reference, the access authorization is provided by an access authorization made up of a subject, object, action, sign, and type columns. When a client

wishes to access an object, the path expression is read from the table. Using Algorithm 6 on page 189, the computer view reads in the data from the access authorization table to determine the view to be returned to a user. The sign indicates a denial or allowance of access by a subject to an object indicated by the path expression. The data from the access authorization table is read in to be executed by the algorithm, and resembles an executable statement. Therefore, Damiani teaches that "access authorization" is an executable statement.

b. Applicant's argument is stated as Damiani discloses an access authorization as both a value expression and the access control rule recited in claim 1, and cannot be construed as disclosing both elements of claim 1.

In response to the argument, Examiner respectfully disagrees. As outlined above, the value expression is disclosed in Damiani is being composed of the subject and sign column of the table, which are read into an algorithm to determine the view given to a user, based on access authorization. The access authorization table controls the access control policy of the system, and within the access authorization table, each row represents an access control rule each subject, or client, follows with respect to access authorization. The value expression is disclosed above to be the individual data points within the table, while the access control rule is disclosed to be a row of the access authorization table determining access rules for a subject. Therefore, Damiani discloses the access authorization table being an access control policy of claim 1, composed of rows of access control rules and containing value expressions to be executed by an algorithm to determine access authorization.

(November 14, 2006 final Office action, pgs. 15-17).

Based on the Examiner's comments, at first it appears that the Examiner is construing the "+" or "-" signs under the "Sign" column in the "access authorizations" table shown in Figure 5 of Damiani as disclosing the "value expression" recited in claim 1. The Examiner then appears to be construing the "Compute-view algorithm" shown in Figure 6 of Damiani as disclosing the "value expression" recited in claim 1. However, the Examiner goes further and now appears to be construing the reading of the "+" or "-" signs under the "Sign" column in the "access authorizations" table shown in Figure 5 of Damiani into the "Compute-view algorithm" shown in Figure 6 of Damiani during execution as disclosing the "value expression" recited in claim 1.

Appellant respectfully submits that none of the above can be construed as disclosing the "value expression" recited in claim 1. In particular, although the Examiner is entitled to a reasonably broad interpretation of the claim terms, the Examiner cannot select an interpretation that is contrary to the accepted meaning of a term by those of ordinary skill in the art. "The broadest reasonable interpretation of the claims must . . . be consistent with the interpretation that those skilled in the art would reach," M.P.E.P. § 2111, citing *In re Cortright*, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999).

Those skilled in the art would not construe the "+" or "-" signs under the "Sign" column in the authorization tables shown in Figure 5 of Damiani as disclosing the "value expression" recited in claim 1 because no one of ordinary skill in the art would interpret "+" or "-" signs to be an "executable statement," which is what the "value expression" in claim 1 has been defined as.

Additionally, the "Compute-view algorithm" shown in Figure 6 of Damiani cannot be construed as disclosing the "value expression" recited in claim 1 because the "Compute-view algorithm" is not specific to any path. In contrast, "a value expression [is generated] for each path" in claim 1; in other words, each path has its own particular "value expression" in claim 1 (an example of which is illustrated in Figure 6 of the present application).

Further, the mere reading of the "+" or "-" signs under the "Sign" column in the "access authorizations" table shown in Figure 5 of Damiani into the "Compute-view algorithm" shown in Figure 6 of Damiani during execution does not magically transform the "+" or "-" signs or the "Compute-view algorithm" into the "value expression" recited in clam 1. Specifically, as clearly illustrated in Figure 8 of Damiani, during execution the "Compute-view algorithm," the access authorizations for all nodes in the document requested by the user are evaluated. Thus, even

during execution, the "Compute-view algorithm" is not specific to a particular path, i.e., a particular node.

Therefore, Damiani fails to disclose, teach, or suggest "generating a value expression for each path based on at least one of the plurality of access control rules, wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document," as recited in claim 1.

(A)(ii) The Examiner has not established anticipation under 35 U.S.C. § 102

Anticipation under 35 U.S.C. § 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention. (*See, e.g.*, Electro Med. Sys. S.A. v. Cooper Life Sciences, 34 F.3d 1048, 32 U.S.P.Q.2d 1017, 1019 (Fed. Cir. 1994)). The Examiner has failed to show that the element discussed above is disclosed in Damiani.

Therefore, claim 1, and the claims that depend therefrom, are not anticipated by Damiani. Given that claims 11, 21, 30, 33, and 36-37 each recite elements similar to those of claim 1, claims 11, 21, 30, 33, and 36-37, and the claims that depend therefrom, are not anticipated by Damiani for at least the same reasons.

CONCLUSION

On the basis of the above remarks, Appellant respectfully submits that the final rejection should be reversed.

Respectfully submitted,
SAWYER LAW GROUP LLP

Dated: June 12, 2006

/Erin C. Ming/
Erin C. Ming
Attorney for Appellant
Reg. No. 47,797
(650) 475-1449

APPENDIX OF CLAIMS

1. (Previously Presented) A method for controlling access to structured documents, the method comprising the steps of:

(a) providing an access control policy for a structured document comprising a plurality of nodes, wherein the access control policy comprises a plurality of access control rules;

(b) generating a path for each of the plurality of nodes in the structured document; and

(c) generating a value expression for each path based on at least one of the plurality of access control rules,

wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

2. (Previously Presented) The method of claim 1, wherein the value expression indicates who is granted or denied access to the corresponding path associated with the node.

3. (Original) The method of claim 1 further comprising:

(d) storing each path and the corresponding value expression in a table.

4. (Original) The method of claim 3 further comprising:

(e) compiling each value expression prior to storing step (d).

5. (Original) The method of claim 4 further comprising:

(f) receiving a query from a user, wherein the query requests access to a node in the document;

(g) executing the query;

(h) evaluating the value expression corresponding to the path associated with the requested node;

(i) displaying data associated with the requested node if the value expression grants access to the user; and

(j) hiding data associated with the requested node if the value expression denies access to the user.

6. (Original) The method of claim 5, wherein the evaluating step (h) is performed during a run time.

7. (Original) The method of claim 1, wherein generating step (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path.

8. (Original) The method of claim 3, further comprising:

(e) replacing the value expression for a path associated with a node with a reference notation if the value expression is identical to that for a path associated with the node's parent, thereby eliminating repeated value expressions in the table.

9. (Original) The method of claim 1, wherein the providing step (a) comprises:

(a1) writing the plurality of access control rules; and

(a2) validating the plurality of access control rules such that the resulting rules are syntactically and logically valid.

10. (Original) The method of claim 1, wherein the structured document is written in Extensible Markup Language.

11. (Previously Presented) A computer readable medium encoded with a computer program for controlling access to structured documents, the computer program comprising instructions for:

(a) providing an access control policy for a structured document comprising a plurality of nodes, wherein the access control policy comprises a plurality of access control rules;

(b) generating a path for each of the plurality of nodes in the structured document; and

(c) generating a value expression for each path based on at least one of the plurality of access control rules,

wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

12. (Previously Presented) The computer readable medium of claim 11, wherein the value expression indicates who is granted or denied access to the corresponding path associated with the node.

13. (Original) The computer readable medium of claim 11 further comprising:

(d) storing each path and the corresponding value expression in a table.

14. (Original) The computer readable medium of claim 13 further comprising:

(e) compiling each value expression prior to storing instruction (d).

15. (Original) The computer readable medium of claim 14 further comprising:

(f) receiving a query from a user, wherein the query requests access to a node in the document;

(g) executing the query;

(h) evaluating the value expression corresponding to the path associated with the requested node;

(i) displaying data associated with the requested node if the value expression grants access to the user; and

(j) hiding data associated with the requested node if the value expression denies access to the user.

16. (Original) The computer readable medium of claim 15, wherein the evaluating instruction (h) is performed during a run time.

17. (Original) The computer readable medium of claim 11, wherein generating instruction (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules associated with each path into a statement indicating who is granted and denied access to the path.

18. (Original) The computer readable medium of claim 13, further comprising:

(e) replacing the value expression for a path associated with a node with a reference notation if the value expression is identical to that for a path associated with the node's parent, thereby eliminating repeated value expressions in the table.

19. (Original) The computer readable medium of claim 11, wherein the providing instruction (a) comprises:

(a1) writing the plurality of access control rules; and

(a2) validating the plurality of access control rules such that the resulting rules are syntactically and logically valid.

20. (Original) The computer readable medium of claim 11, wherein the structured document is written in Extensible Markup Language.

21. (Previously Presented) A computer system for controlling access to structured documents, the computer system comprising:

a database management system implemented on the computer system, the database management system comprising

an access control policy for a structured document, wherein the structured document comprises a plurality of nodes and the access control policy comprises a plurality of access control rules, and

an access control mechanism configured to

generate a path for each of the plurality of nodes in the structured document and

generate a value expression for each path based on at least one of the plurality of access control rules,

wherein the value expression is an executable statement utilized by the database management system during access control evaluation to determine whether a user is allowed to access a node in the structured document.

22. (Previously Presented) The computer system of claim 21, wherein the value expression indicates who is granted or denied access to the corresponding path associated with the node.

23. (Previously Presented) The computer system of claim 21, wherein the access control mechanism is configured to store each path and the corresponding value expression in a table.

24. (Previously Presented) The computer system of claim 23, wherein the database management system further comprises a compiler configured to compile each value expression prior to storage of the value expression in the table.

25. (Previously Presented) The computer system of claim 24, wherein the database management system is configured to receive a query from a user, wherein the query requests access to a node in the document, to execute the query, to evaluate the value expression corresponding to the path associated with the requested node, to display data associated with the requested node if the value expression grants access to the user, and to hide data associated with the requested node if the value expression denies access to the user.

26. (Previously Presented) The computer system of claim 25, wherein access control evaluation is performed during a run time.

27. (Previously Presented) The computer system of claim 21, wherein the access control mechanism comprises:

a translator for normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path, and for propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

a value expression generator for transforming each of the at least one access control rules associated with each path into a statement indicating who is granted and denied access to the path.

28. (Previously Presented) The computer system of claim 21, wherein the access control rules are syntactically and logically valid.

29. (Previously Presented) The computer system of claim 21, wherein the structured document is written in Extensible Markup Language.

30. (Previously Presented) A method for controlling access to structured documents, the method comprising the steps of:

(a) providing an access control policy for a structured document comprising a plurality of nodes, wherein the access control policy comprises a plurality of access control rules;

(b) generating a path for each of the plurality of nodes in the structured document;

(c) generating a value expression for each path based on at least one of the plurality of access control rules, wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node; and

(d) storing each path and the corresponding value expression in a table;

wherein the value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

31. (Original) The method of claim 30 further comprising:

(e) receiving a query from a user, wherein the query requests access to a node in the document;

(f) executing the query;

(g) evaluating the value expression corresponding to the path associated with the requested node during a run time;

(h) displaying data associated with the requested node if the value expression grants access to the user; and

(i) hiding data associated with the requested node if the value expression denies access to the user.

32. (Original) The method of claim 30, wherein generating step (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path.

33. (Previously Presented) A computer readable medium encoded with a computer program for controlling access to structured documents, the computer program comprising instructions for:

(a) providing an access control policy for a structured document comprising a plurality of nodes, wherein the access control policy comprises a plurality of access control rules;

(b) generating a path for each of the plurality of nodes in the structured document;

(c) generating a value expression for each path based on at least one of the plurality of access control rules, wherein the value expression is an executable statement indicating who is granted or denied access to the corresponding path associated with the node; and

(d) storing each path and the corresponding value expression in a table;

wherein the value expression is utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

34. (Original) The computer readable medium of claim 33 further comprising:

(e) receiving a query from a user, wherein the query requests access to a node in the document;

(f) executing the query;

(g) evaluating the value expression corresponding to the path associated with the requested node during a run time;

(h) displaying data associated with the requested node if the value expression grants access to the user; and

(i) hiding data associated with the requested node if the value expression denies access to the user.

35. (Original) The computer readable medium of claim 33, wherein generating instruction (c) further comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path.

36. (Previously Presented) A method for controlling access to structured documents, the method comprising the steps of:

(a) providing an access control policy for a structured document comprising a plurality of nodes, wherein the access control policy comprises a plurality of access control rules;

(b) generating a path for each of the plurality of nodes in the structured document;

(c) generating a value expression for each path based on at least one of the plurality of access control rules, wherein the generating step comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path; and

(d) storing each path and the corresponding value expression in a table;

wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

37. (Previously Presented) A computer readable medium encoded with a computer program for controlling access to structured documents, the computer program comprising instructions for:

(a) providing an access control policy for a structured document comprising a plurality of nodes, wherein the access control policy comprises a plurality of access control rules;

(b) generating a path for each of the plurality of nodes in the structured document;

(c) generating a value expression for each path based on at least one of the plurality of access control rules, wherein the generating step comprises:

(c1) normalizing each of the access control rules into a format comprising a head, a path and a condition, wherein the condition indicates who is granted or denied access to the path and under what circumstances;

(c2) propagating each of the plurality of access control rules through each path such that access to each path is defined by at least one access control rule; and

(c3) transforming each of the at least one access control rules affecting each path into a statement indicating who is granted and denied access to the path; and

(d) storing each path and the corresponding value expression in a table;

wherein the value expression is an executable statement utilized during access control evaluation to determine whether a user is allowed to access a node in the structured document.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None